باب نمبر 4

ڈیٹا اور رازداری کا معاملہ

DATA AND PRIVACY

(مشقی کثیر الانتخابی سوالات)

01۔ درج ذیل میں سے کیا سافٹ پائیریسی کی اقسام میں شامل ہے؟
(a) سافٹ لفٹنگ (b) ذمہ داری (c) کلائنٹ سرور اوور یوز (d) آن لائن پائیریسی

02۔ درج ذیل میں سے کون سا سائبر کرائم نہیں ہے؟
(a) ہیکنگ (b) فشنگ کرائم (c) شناخت کی چوری (d) ڈیکرپشن

03۔ درج ذیل میں سے کون سا عمل فشنگ ای میل کی خوبی نہیں ہے؟
(a) سرکاری ڈیٹا کی خلاف ورزی کی اطلاع (b) ای میل اکاؤنٹ اپ ڈیٹ
(c) آئی ٹی یاد دہانی (d) اصل ویب سائٹ کی ڈومین

04۔ درج ذیل میں سے فشنگ ویب سائٹ کی خوبی نہیں ہے:
(a) اصل ویب سائٹ جیسی ڈومین (b) زائرین کو جمع کرنے کے لیے فارم کا استعمال
(c) ویب مواد سے اصل لنک (d) ای میل اکاؤنٹ اپ ڈیٹس

05۔ درج ذیل میں سے کون سی اچھے پاس ورڈ کی خوبی نہیں ہے؟
(a) آٹھ حروف طوالت (b) یوزر نیم پر مشتمل نہ ہو
(c) بڑے حروف پر مشتمل ہے (d) پاس ورڈ صرف آپ کے نام پر مشتمل ہے

(اضافی کثیر الانتخابی سوالات)

01۔ ضرر پہنچانے والے صارفین سے ڈیٹا کی حفاظت کرنا کہلاتا ہے:
(a) رازداری (b) پوشیدگی
(c) ڈیٹا یا معلومات کی رازداری (d) ان میں کوئی نہیں

02۔ اگر ہمارے پاس دوسروں کا ڈیٹا ہے تو یہ ہماری ۔۔۔۔۔۔۔ ذمہ داری ہے کہ ہم اسے محفوظ رکھیں۔
(a) اخلاقی (b) معاشی (c) دینی (d) دنیاوی

03۔ کوئی کاپی رائٹ کے تحفظات نہیں ہوتے:
(a) سافٹ ویئر پائیریسی میں (b) سافٹ لفٹنگ میں
(c) Open Source Software میں (d) جعل سازی میں

04۔ کچھ سافٹ ویئر کمپنیاں سافٹ ویئر کو خفیہ متن کے ساتھ فروخت کرتی ہیں جسے اس سافٹ ویئر کی ۔۔۔۔۔ کہتے ہیں۔
(a) کمانڈ (b) سٹیٹمنٹ (c) کی (d) ان میں کوئی نہیں

05۔ کسی دوسرے سے ایپلی کیشن سافٹ ویئر کی کاپی لے کر انسٹال کرنا:
(a) سافٹ لفٹنگ (b) کلائنٹ سرور اوور یوز (c) ہارڈ ڈسک لوڈنگ (d) جعل سازی

06۔ تمام حفاظتی نظام کی بنیاد۔۔۔۔۔۔۔۔۔۔۔پر قائم ہے۔
(a) اخلاقی اصولوں (b) معاشی اصولوں (c) سائنسی اصولوں (d) دنیاوی اصولوں

07۔ پائریسی کا مطلب۔۔۔۔۔۔۔۔تیار کرنا ہے۔
(a) قانونی نقلیں (b) غیر قانونی نقلیں (c) درست نقلیں (d) غلط نقلیں

08۔ کسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم یا استعمال ہے:
(a) سافٹ ویئر پائریسی (b) سافٹ لفٹنگ (c) جعل سازی (d) شیئرنگ

09۔ صرف ان لوگوں کو فراہم کی جاتی ہے جو اس سافٹ ویئر کو خریدتے ہیں:
(a) پائریسی کی اجازت (b) سافٹ لفٹنگ کی اجازت
(c) سافٹ ویئر ڈسکرپشن (d) سافٹ ویئر کی

10۔ تجدید شدہ یا نئے کمپیوٹر پر غیر مجاز شدہ سافٹ ویئر کی کاپیاں انسٹال اور فروخت کرنا:
(a) سافٹ لفٹنگ (b) کلائنٹ سرور اوور یوز (c) ہارڈ ڈسک لوڈنگ (d) جعل سازی

11۔ عموماً غیر قانونی سافٹ ویئرز ڈاؤن لوڈ کرنا شامل ہے:
(a) آن لائن پائریسی میں (b) کلائنٹ سرور اوور یوز میں
(c) ہارڈ ڈسک لوڈنگ میں (d) جعل سازی میں

12۔ کسی آئیڈیا کی حفاظت کا ایک طریقہ ہے:
(a) سافٹ لفٹنگ (b) Phishing (c) پیٹنٹ (d) کاپی رائٹ قانون

13۔ وہ راز جو کسی کمپنی کی کامیابی کے لیے نمایاں کردار ادا کریں:
(a) تجارتی راز (b) تخریب کاری (c) پیٹنٹ (d) کاپی رائٹ قانون

14۔ بُرے ارادے سے لکھا گیا کمپیوٹر پروگرام ہے:
(a) مائیکروسافٹ ورڈ (b) اینٹی وائرس (c) وائرس (d) کورل ڈرا

15۔ حاصل کردہ لائسنس کے مقابلے سافٹ ویئر کی مزید کاپیاں انسٹال کرنا:
(a) سافٹ لفٹنگ (b) کلائنٹ سرور اوور یوز (c) ہارڈ ڈسک لوڈنگ (d) جعل سازی

16۔ سافٹ ویئر کی نقلیں تیار کرنے اور بیچنے کے بھی کاپی رائٹ ہوتے ہیں:
(a) سافٹ لفٹنگ (b) کلائنٹ سرور اوور یوز (c) ہارڈ ڈسک لوڈنگ (d) جعل سازی

17۔ بعض اوقات نقصان پہنچانے والے صارف ہمیں اپنا دوست ظاہر کر کے ہماری کچھ خفیہ معلومات حاصل کرنے کی کوشش کرتے ہیں، اسے کہتے ہیں:
(a) سافٹ لفٹنگ (b) فشنگ (c) پیٹنٹ (d) کاپی رائٹ قانون

18۔ کسی بھی آئیڈیا یا چیز کو کاپی نہیں کیا جا سکتا:
(a) سافٹ لفٹنگ (b) فشنگ (c) پیٹنٹ (d) کاپی رائٹ قانون

19۔ کمپیوٹر سسٹم پر ایک سنگین حملہ ہے:
(a) تجارتی راز (b) تخریب کاری (c) پیٹنٹ (d) کاپی رائٹ قانون

20۔ معلومات کو تبدیل یا تباہ کر سکتا ہے یا قیمتی ڈیٹا سے چھیڑ چھاڑ کر سکتا ہے:
(a) مائیکروسافٹ ورڈ (b) اینٹی وائرس (c) وائرس (d) کورل ڈرا

21۔ ڈیٹا کو نہ پڑھے جا سکنے والی شکل میں تبدیل کرنا ہے:

(a) کوکیز (b) ہیکرز (c) خفیہ کاری (d) اِن کوڈنگ

22۔ ہمارے ڈیٹا کو ہیکرز سے بچانے میں مدد کرتی ہے:

(a) کوکیز (b) وائرس (c) خفیہ کاری (d) اِن کوڈنگ

23۔ ایک ایسا عمل ہے جس کی مدد سے ڈیٹا کی اِن کوڈنگ کی جاتی ہے:

(a) کوکیز (b) ہیکرز (c) خفیہ کاری (d) اِن کوڈنگ

24۔ کمپیوٹر ماہر جو ڈیٹا چوری کر سکتا ہے اسے کہتے ہیں:

(a) رائٹر (b) ہیکر (c) پروگرامر (d) اینالسٹ

25۔ یہ ڈیٹا کو غیر قانونی رسائی سے محفوظ رکھتی ہے:

(a) کوکیز (b) ہیکر (c) خفیہ کاری (d) اِن کوڈنگ

26۔ ڈیٹا کو سکیورٹی فراہم کرنے کے لیے۔۔۔۔۔۔۔۔ایک اہم طریقہ ہے۔

(a) کوکیز (b) ہیکنگ (c) خفیہ کاری (d) اِن کوڈنگ

27۔ صرف معلومات چوری نہیں کرتے ہیں وہ دھوکا دینے کے لیے ڈیٹا کو تبدیل کر کے بھی فائدہ اٹھا سکتے ہیں:

(a) کوکیز (b) ہیکرز (c) خفیہ کاری (d) اِن کوڈنگ

28۔ تمام آلات میں ڈیٹا محفوظ کرتے وقت یہاں تک کہ منتقل کرتے وقت ان کی حفاظت میں مدد دیتی ہے:

(a) کوکیز (b) ہیکنگ (c) خفیہ کاری (d) اِن کوڈنگ

29۔ خفیہ کاری کی اہمیت۔۔۔۔۔۔۔۔نکات میں بیان کی جا سکتی ہے۔

(a) دو (b) تین (c) چار (d) پانچ

30۔ حساس ڈیٹا سمیت افراد کی ذاتی معلومات کی بھی حفاظت کرتی ہے:

(a) کوکیز (b) ہیکنگ (c) خفیہ کاری (d) اِن کوڈنگ

31۔ اضافی حفاظتی اقدامات جیسا کہ۔۔۔۔۔۔۔۔غیر مجاز صارفین کو روکنے میں مدد کرتے ہیں۔

(a) کوکیز (b) اِن کوڈنگ

(c) خفیہ کاری (d) اعلیٰ درجے کی تصدیق

32۔ متبادل سازی کے طریقے ہیں:

(a) دو (b) تین (c) چار (d) پانچ

33۔ متبادل سازی۔۔۔۔۔۔۔۔کا ایک طریقہ ہے جس میں اصل متن کے حروف دوسرے حروف کے ساتھ تبدیل کر دیے جاتے ہیں۔

(a) کوکیز (b) ہیکنگ (c) خفیہ کاری (d) اِن کوڈنگ

34۔ رومن سلطنت کے عروج میں اہم کردار ادا کیا:

(a) جارج بولی نے (b) ہٹلر نے (c) افلاطون نے (d) سیزر نے

35۔ ہم ہر حروفِ تہجی کو تحریر کرتے وقت دوسرے حروف سے تبدیل کر دیتے ہیں:

(a) سیزر سائیفر طریقے میں (b) وگینیر سائیفر طریقے میں

(c) a اور b (d) ان میں کوئی نہیں

36۔ سیزر ایک۔۔۔۔۔۔۔۔سیاست دان اور فوجی جنرل تھا۔

(a) چینی (b) رومن (c) امریکی (d) روسی

37۔ سیزر نے اپنے فوجیوں اور جرنیلوں کو پیغامات بھیجنے کے لیے ایک خفیہ کاری کا طریقہ استعمال کیا۔ اس لیے اس طریقے کو۔۔۔۔۔۔۔۔ کہا جاتا ہے۔
(a) سیزر سائیفر (b) وگینیر سائیفر (c) a اور b (d) ان میں کوئی نہیں

38۔ سادہ عبارت کے حروف کو تبدیل کرنے کے لیے ایک ٹیبل کا استعمال کیا جاتا ہے جسے وگینیر سائیفر ٹیبل کہتے ہیں:
(a) سیزر سائیفر میں (b) وگینیر سائیفر میں (c) a اور b (d) ان میں کوئی نہیں

39۔ ہمارے پاس ایک متبادل کلید ہوتی ہے جسے سادہ عبارت کے ساتھ ملا دیا جاتا ہے جس سے سائیفر ٹیکسٹ بنتا ہے:
(a) سیزر سائیفر طریقے میں (b) وگینیر سائیفر طریقے میں
(c) a اور b (d) ان میں کوئی نہیں

40۔ ایک دوسرا متبادل سائیفر ہے:
(a) سیزر سائیفر (b) وگینیر سائیفر (c) a اور b (d) ان میں کوئی نہیں

41۔ چھبیس قطاروں اور چھبیس کالموں پر مشتمل ہے:
(a) ٹریس ٹیبل (b) وگینیر سائیفر ٹیبل (c) معلوماتی ٹیبل (d) ٹروتھ ٹیبل

42۔ اگر کلید کے حروف کی تعداد عبارت کے حروف سے کم ہو تو ہم کلید کے حروف کو شروع سے دوبارہ لکھیں گے، اس طریقے کو کہتے ہیں:
(a) اِنٹیرم سائیفر ٹیکسٹ (b) سائیفر ٹیکسٹ (c) a اور b (d) ان میں کوئی نہیں

43۔ پڑھنے کے لیے کرپٹو گرافک کیز کا استعمال کیا جاتا ہے:
(a) خفیہ کاری پیغام کو (b) پاس ورڈز کو (c) الگورتھم کو (d) خفیہ کاری پیغام کو

44۔ ایک سسٹم تک رسائی حاصل کرنے کے لیے تصدیق کے طور پر استعمال کیا جاتا ہے:
(a) خفیہ کاری پیغام کو (b) پاس ورڈز کو (c) الگورتھم کو (d) خفیہ کاری پیغام کو

45۔ اچھے۔۔۔۔۔۔۔۔ اندازہ لگانا اور اس میں دراڑ پیدا کرنا مشکل ہونا چاہیے۔
(a) پیغام کا (b) پاس ورڈ کا (c) الگورتھم کا (d) ان میں کوئی نہیں

46۔ سائبر کرائم کی ایک عام شکل ہے:
(a) ٹرانزیکشن فراڈ (b) ایڈوانس فیس فراڈ (c) ہیکنگ (d) شناخت کی چوری

47۔ غیر قانونی طور پر کسی دوسرے شخص کے کمپیوٹر تک رسائی حاصل کرنا کہلاتا ہے:
(a) ٹرانزیکشن فراڈ (b) ایڈوانس فیس فراڈ (c) ہیکنگ (d) شناخت کی چوری

48۔ سائبر کرائم کے خلاف پاکستان کی قانون نافذ کرنے والی ایجنسی ہے:
(a) نیشنل رسپونس فورس (b) نیشنل رسپونس کورٹ
(c) نیشنل رسپونس بیورو (d) نیشنل رسپونس سینٹر

49۔ ایک جرم جس میں کمپیوٹر نیٹ ورک یا آلات استعمال کیے جاتے ہیں اسے کہتے ہیں:
(a) عام کرائم (b) کمپیوٹر کرائم (c) سائبر کرائم (d) سٹریٹ کرائم

50۔ آن لائن میدان میں ایک عام جرم ہے:
(a) مالی دھوکادہی (b) ایڈوانس فیس فراڈ (c) ہیکنگ (d) شناخت کی چوری

51۔ سائبر جرم کی ایک عام قسم ہے:
(a) سپائی ویئر (b) پائریسی (c) پاس ورڈ (d) کرپٹو گرافک کیز

52۔ NRC مخفف ہے:

(a) National Response College for Cyber Crime
(b) National Response Court for Cyber Crime
(c) National Response Centre for Cyber Crime
(d) ان میں کوئی نہیں

☆☆☆☆☆

(مشقی مختصر جوابی سوالات)

4.3۔ ان سوالوں کا جواب دیں۔

سوال (i): سائیفر ٹیکسٹ کی وضاحت کریں۔

جواب: اِن کوڈنگ کے ذریعہ تبدیل کیے گئے ڈیٹا کو سائیفر ٹیکسٹ کہتے ہیں۔

سوال (ii): ہمیں ایک انسٹالیشن کی کی ضرورت کیوں ہوتی ہے جبکہ ایک سافٹ ویئر کو پاس ورڈ کے ساتھ محفوظ کیا جاسکتا ہے؟

جواب: سافٹ ویئر کمپنیاں اپنے سافٹ ویئر کو خفیہ متن کے ساتھ فروخت کرتی ہیں جسے اس سافٹ ویئر کی کی کہتے ہیں۔ یہ کی سافٹ ویئر انسٹال کرتے وقت داخل کی جاتی ہے تاکہ کوئی غیر مجاز شخص سافٹ ویئر انسٹال نہ کرسکے جبکہ پاس ورڈ سے انسٹال کیے گئے سافٹ ویئر کو محفوظ کیا جاسکتا ہے کہ کوئی غیر مجاز شخص اس سافٹ ویئر کو استعمال نہ کرسکے۔

سوال (iii): DOS اٹیک کی وضاحت کریں۔

جواب: DOS سائبر اٹیک کی ایک قسم ہے جس میں کسی مشین یا کمپیوٹر کو اس کے اصل صارف کے لیے بیکار کر دیتے ہیں۔ اس کا مطلب یہ ہے کہ وہ سروس معطل ہوگئی ہے۔

سوال (iv): کیپچا کو ویب سائٹ پر دینے کی وجہ کیا ہے؟

جواب: ویب سائٹ کو DOS اٹیک سے بچانے کے لیے کیپچا کا طریقہ استعمال کیا جاتا ہے۔ کیپچا ایک ٹیڑھے میڑھے حروف پر مشتمل ایک ٹیکسٹ ہوتی ہے جسے صرف انسان ہی سمجھ سکتا ہے روبوٹ نہیں سمجھ سکتا۔

سوال (v): پیٹنٹ کیا ہے اور ہمیں اسے رجسٹر کرنے کی ضرورت کیوں ہے؟

جواب: ایک طریقہ جو کسی آئیڈیا کی حفاظت کرتا ہے، پیٹنٹ کہلاتا ہے۔

مثال: اگر آپ کسی فیلڈ میں تحقیق کر رہے ہیں اور آپ کے پاس کوئی آئیڈیا ہے تو آپ کو چاہیے کہ آئیڈیا کا پیٹنٹ حاصل کرلیں۔ یہ دوسروں کو اس آئیڈیا کی بنیاد پر کچھ ایجاد کرنے اور فروخت کرنے سے روکنے کا آپ کو حق دیتا ہے۔

(اضافی مختصر جوابی سوالات)

سوال 1: ڈیٹا کی رازداری سے کیا مراد ہے؟

جواب: نقصان پہنچانے والے صارفین سے ڈیٹا کی حفاظت کرنا ڈیٹا کی رازداری کہلاتا ہے۔ اسے معلومات کی رازداری بھی کہتے ہیں۔

مثال: ای میل اکاؤنٹ بناتے ہوئے، آن لائن خریداری کرتے ہوئے ایک ہسپتال کا دورہ اور اسکول میں داخلہ لیتے ہوئے ہم یہ خیال کرتے ہیں کہ ہماری فراہم کردہ معلومات کسی کو نہیں بتائی جائیں گی، یہ ڈیٹا کی رازداری ہے۔

سوال 2: ڈیٹا سیکیورٹی کے چند نام لکھیں۔

جواب: ڈیٹا سیکیورٹی کے چند نام درج ذیل ہیں:

(i) رازداری اور پوشیدگی (ii) دھوکہ دہی اور غلط استعمال (iii) پیٹنٹ
(iv) کاپی رائٹ (v) تجارتی راز (vi) تخریب کاری

سوال3: رازداری اور پوشیدگی سے کیا مراد ہے؟

جواب: دوسروں کا ڈیٹا محفوظ رکھنا در حقیقت دوسروں کی حفاظت کرنا ہے۔ ہر وہ تنظیم جس کو ڈیٹا منتقل کیا جاتا ہے ڈیٹا کی رازداری اور تحفظ اس کی ذمہ داری ہے۔

مثال: اگر کوئی بینک کسی بھی کاروباری حریف کو اپنی بینکنگ ٹرانزیکشن کی معلومات میں شریک کرتا ہے تو یہ میرے کاروبار کو نقصان پہنچا سکتا ہے۔ اس لیے بینک کو ہمارا ڈیٹا خفیہ طور پر رکھنا چاہیے۔

سوال4: پائریسی کی تعریف کریں۔

جواب: پائریسی کا مطلب مالک کی اجازت کے بغیر اس کے ڈیٹا کی غیر قانونی اور غیر مجاز شدہ نقول تیار کرنا ہے۔ ڈیٹا ایک کتاب، سافٹ ویئر، مووی، شاعری، مصوری یا کاپی رائٹ قانون کے تحت محفوظ شدہ کوئی دوسرا کام ہو سکتا ہے۔

سوال5: سافٹ ویئر پائریسی کی تعریف کریں۔

جواب: کسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم یا استعمال کرنا سافٹ ویئر پائریسی کہلاتا ہے۔

سوال6: سافٹ ویئر پائریسی کی اقسام کون کون سی ہیں؟ نام تحریر کریں۔

جواب: سافٹ ویئر پائریسی کی مندرجہ ذیل اقسام ہیں:

(i) سافٹ لفٹنگ (ii) کلائنٹ سرور اوور یوز (iii) ہارڈ ڈسک لوڈنگ
(iv) جعل سازی (v) آن لائن پائریسی

سوال7: سافٹ لفٹنگ کیا ہے؟

جواب: سافٹ لفٹنگ قانونی طور پر لائسنس یافتہ سافٹ ویئر پروگرام کی غیر مجاز کاپی یا انسٹالیشن ہے۔ کسی دوسرے ایپلی کیشن سافٹ ویئر کی کاپی لینا اور انسٹال کرنا بھی سافٹ لفٹنگ کہلاتا ہے۔

سوال8: کلائنٹ سرور اوور یوز سے کیا مراد ہے؟

جواب: کلائنٹ سرور اوور یوز کا مطلب ہے کہ لیے گئے سافٹ ویئر کے لائسنس سے بڑھ کر اس کی کاپیاں انسٹال کرنا ہے۔

سوال9: ہارڈ ڈسک لوڈنگ سے کیا مراد ہے؟

جواب: ہارڈ ڈسک لوڈنگ کا مطلب سافٹ ویئر کی غیر مجاز کاپیاں نئے کمپیوٹر پر انسٹال کرنا یا فروخت کرنا ہے۔

سوال10: جعل سازی سے کیا مراد ہے؟

جواب: کاپی رائٹ پروگرام کو نقل اور فروخت کرنا جعل سازی کہلاتا ہے۔

سوال11: آن لائن پائریسی کیا ہے؟

جواب: غیر قانونی سافٹ ویئر ڈاؤن لوڈ کرنا آن لائن پائریسی کہلاتا ہے۔ انٹرنیٹ سے ایک کاپی رائٹ گانا ڈاؤن لوڈ کرنا آن لائن پائریسی کی ایک مثال ہے۔

سوال12: "دھوکہ دہی اور غلط استعمال" سے کیا مراد ہے؟

جواب: کسی غیر مجاز سرگرمی کے مقصد سے کمپیوٹر کا استعمال دھوکہ دہی یا غلط استعمال ہے۔

سوال13: فشنگ کیا ہے؟

جواب: بعض اوقات نقصان پہنچانے والے صارف ہمیں اپنا دوست ظاہر کر کے ہماری کچھ خفیہ معلومات حاصل کرنے کی کوشش کرتے ہیں۔ اسے فشنگ کہتے ہیں۔

سوال14: پیٹنٹ کی تعریف کریں اور مثال دیں۔

جواب: ایک طریقہ جو کسی آئیڈیا کی حفاظت کرتا ہے، پیٹنٹ کہلاتا ہے۔

مثال: اگر آپ کسی فیلڈ میں تحقیق کر رہے ہیں اور آپ کے پاس کوئی آئیڈیا ہے تو آپ کو چاہیے کہ آئیڈیا کا پیٹنٹ حاصل کر لیں۔ یہ دوسروں کو اس آئیڈیا کی بنیاد پر کچھ ایجاد کرنے اور فروخت کرنے سے روکنے کا آپ کو حق دیتا ہے۔

سوال15: کاپی رائٹ قانون سے کیا مراد ہے؟

جواب: کاپی رائٹ قانون کے مطابق کسی بھی آئیڈیا یا چیز کو کاپی نہیں کیا جا سکتا۔ کاپی رائٹ کا نشان "©" ہے۔

مثال: سافٹ ویئر جیسے مائیکروسافٹ ورڈ اور مائیکروسافٹ ونڈوز کاپی رائٹ کے تحت محفوظ ہیں لہٰذا ہم ان کی کاپی نہیں کر سکتے۔

سوال16: تجارتی راز کیا ہوتے ہیں؟

جواب: تجارتی راز سے مراد وہ راز جو کسی کمپنی کی کامیابی کے لیے نمایاں کردار ادا کریں۔ یہ راز کمپنی کے لیے بہت اہم ہوتے ہیں۔ کمپیوٹر سائنس کے شعبہ میں تجارتی راز پوشیدہ رکھنا بہت اہم ہیں۔ اس صورتِ حال میں جب ایک سے زائد سوفٹ ویئر کمپنیاں ایک ہی قسم کی مصنوعات تیار کرتی ہوں اور ان میں کسی ایک کو دوسری کمپنی پر برتری حاصل ہو سکتی ہے۔

مثال: بہت سی کمپنیاں سمارٹ فون تیار کر رہی ہیں لیکن ان میں کچھ کمپنیوں کو دوسری کمپنیوں پر برتری حاصل ہے۔

سوال17: تخریب کاری کی تعریف کریں۔

جواب: تخریب کاری کمپیوٹر سسٹم پر ایک سنگین حملہ ہے۔ کچھ نقصان پہنچانے والے صارف دور بیٹھے ہوئے ہی اس سسٹم پر حملہ کر سکتے ہیں۔ کسی مفت سافٹ ویئر کے ذریعے وائرس بھیج سکتا ہے۔ یہ معلومات کو تبدیل یا تباہ کر سکتا ہے یا قیمتی ڈیٹا سے چھیڑ چھاڑ کر سکتا ہے۔

سوال18: کمپیوٹر وائرس کیا ہوتا ہے؟

جواب: وائرس بُرے ارادے سے لکھا گیا کمپیوٹر پروگرام ہے۔ یہ معلومات کو تبدیل یا تباہ کر سکتا ہے یا قیمتی ڈیٹا سے چھیڑ چھاڑ کر سکتا ہے۔

مثالیں: وائرس کی چند مثالیں درج ذیل ہیں:

(i) Morris Worm　(ii) Nimda　(iii) SQL Slammer
(iv) MyDoom　(v) Sasser/Netsky　(vi) Code Red

سوال19: خفیہ کاری کی تعریف کریں۔

جواب: خفیہ کاری ایک ایسا عمل ہے جس کی مدد سے ڈیٹا کی ان کوڈنگ کی جاتی ہے۔ اس طرح صرف مجاز افراد ہی اسے پڑھ سکتے ہیں۔

سوال20: ہیکر کون ہوتا ہے؟

جواب: کمپیوٹر ماہر جو ڈیٹا چوری کر سکتا ہے (جب ڈیٹا ایک مقام سے دوسرے مقام تک جائے) اسے ہیکر کہتے ہیں۔

سوال21: خفیہ کاری ڈیٹا کو کیسے ہیکرز سے تحفظ فراہم کرتی ہے؟

جواب: ہیکرز صرف معلومات چوری نہیں کرتے بلکہ وہ دھوکہ دینے کے لیے ڈیٹا کو تبدیل کر کے بھی فائدہ اٹھا سکتے ہیں۔ مثال کے طور پر آن لائن پیسے منتقلی کی بینک ٹرانزیکشن میں وہ ٹارگیٹ اکاؤنٹ نمبر کو تبدیل کر کے دھوکہ دے سکتے ہیں۔ لیکن خفیہ کاری سے ڈیٹا کو ہیکرز سے بچانے میں مدد ملتی ہے۔

سوال22: خفیہ کاری رازداری کی حفاظت کیسے کرتی ہے؟

جواب: خفیہ کاری حساس ڈیٹا سمیت افراد کی ذاتی معلومات کی بھی حفاظت کرتی ہے۔ یہ رازداری کو یقینی بناتی ہے اور مجرموں کو آپ کے ڈیٹا کی نگرانی کم کرنے میں بھی مدد فراہم کرتی ہے۔ اس طرح خفیہ کاری رازداری کی حفاظت کرتی ہے۔

سوال23: خفیہ کاری آلات میں ڈیٹا کی حفاظت کیسے کرتی ہے؟

جواب: ایک سے زیادہ (موبائل) آلات ہماری زندگی کا ایک بڑا حصہ ہیں اور ایک آلہ سے دوسرے آلہ کو حساس ڈیٹا منتقل کرنا ایک خطرناک عمل ہے۔ خفیہ کاری تمام آلات میں ڈیٹا محفوظ کرتے وقت یہاں تک کے منتقل کرتے وقت ان کی حفاظت میں مدد دیتی ہے۔ اضافی حفاظتی اقدامات جیسا کہ اعلیٰ درجے کی تصدیق غیر مجاز صارفین کو روکنے میں مدد کرتے ہیں۔

سوال24: تبادل سازی کے طریقے کی تعریف کریں۔

جواب: متبادل سازی خفیہ کاری کا ایک طریقہ ہے جس میں اصل متن کے حروف دوسرے حروف کے ساتھ تبدیل کر دیے جاتے ہیں۔ یہ متبادل عمل ایک مقررہ وضاحتی نظام کی مدد سے کیا جاتا ہے۔

سوال 25: جولیس سیزر کون تھا؟

جواب: جولیس سیزر ایک رومن سیاست دان اور فوجی جنرل تھا جس نے رومن سلطنت کے عروج میں اہم کردار ادا کیا۔

سوال 26: سیزر سائیفر کا طریقہ کیا ہے؟

جواب: سیزر سائیفر طریقے میں ہم ہر حروف تہجی تحریر کرتے وقت دوسرے حروف سے تبدیل کر دیتے ہیں۔ حروف کی ترتیب میں اصل حروف تہجی کے بائیں یا دائیں کے لیے کچھ طے شدہ نمبر ز ہوتے ہیں۔ مثال کے طور پر معیاری انگریزی حروف تہجی کے "تین حروف دائیں جانب متبادل" سے ہمیں مندرجہ ذیل نتائج حاصل ہوتے ہیں:

ابتدائی حروف: ABCDEFGHIJKLMNOPQRSTUVWXYZ

خفیہ کاری حروف: DEFGHIJKLMNOPQRSTUVWXYZABC

سوال 27: وگینیر سائیفر ٹیبل کیا ہوتا ہے؟

جواب: وگینیر سائیفر ٹیبل ایک دوسرا متبادل سائیفر ہے جس میں سادہ عبارت کے حروف کو تبدیل کرنے کے لیے ایک ٹیبل کا استعمال کیا جاتا ہے۔ جسے وگینیر سائیفر ٹیبل کہتے ہیں۔

سوال 28: وگینیر سائیفر ٹیبل میں کتنی قطاریں اور کالم ہوتے ہیں؟

جواب: وگینیر سائیفر ٹیبل میں 26 قطاریں اور 26 کالم ہوتے ہیں۔

سوال 29: وگینیر سائیفر طریقہ کیا ہوتا ہے؟

جواب: وگینیر سائیفر کے طریقے میں ہمارے پاس ایک متبادل کلید ہوتی ہے جسے سادہ عبارت کے ساتھ ملا دیا جاتا ہے جس سے سائیفر ٹیکسٹ بنتا ہے۔ ہم سادہ عبارت کے ہر حروف کو خفیہ کاری میں تبدیل کرنے کے لیے وگینیر ٹیبل کے کالم میں تلاش کرتے ہیں اور اس کالم میں ہم اس حروف کو تلاش کرتے ہیں جو کلید کے متعلقہ حروف کے سامنے ٹیبل کی قطار میں آرہا ہے۔ ہم یہ عمل جاری رکھتے ہیں جب تک کہ ساری عبارت ختم نہ ہو جائے۔

سوال 30: اینٹریم سائیفر ٹیکسٹ کیا ہے؟

جواب: جب کسی کلید میں خفیہ کردہ متن کے مقابلے میں حروف کی تعداد کم ہوتی ہے تو پھر کلید کے حروف دہرانے کو اینٹریم سائیفر ٹیکسٹ کہتے ہیں۔

سوال 31: کرپٹو گرافک کیز اور پاس ورڈ کے مابین کیا فرق ہے؟

جواب: ان دونوں میں بنیادی فرق یہ ہے کہ پاس ورڈ کو بنانا، پڑھنا اور یاد رکھنا انسانی عمل ہے۔ کچھ سرور کمپیوٹرز پاس ورڈ آپ کے کمپیوٹر پر ہی محفوظ کرتے ہیں۔ اگلی دفعہ استعمال پر یہ ہی پاس ورڈ استعمال کیا جاتا ہے۔ جبکہ کی ایک پیغام کو پروسس کرنے کے لیے کسی کرپٹو گرافک الگورتھم کے ذریعے کوئی سافٹ ویئر یا انسان استعمال کر سکتا ہے۔

سوال 32: اچھے پاس ورڈ کی خصوصیات لکھیں۔

جواب: اچھے پاس ورڈ کی مندرجہ ذیل خصوصیات ہیں:

(i) یہ کم سے کم آٹھ حروف پر مشتمل ہو۔ (ii) یہ آپ کے نام پر مشتمل نہ ہو۔

(iii) یہ مکمل لفظ پر مشتمل نہ ہو۔ (iv) یہ گزشتہ پاس ورڈ سے نمایاں طور پر مختلف ہو۔

(v) یہ بڑے حروف، چھوٹے حروف، نمبرز اور علامات پر مشتمل ہو۔

سوال 33: سائبر کرائم کی تعریف کریں۔

جواب: ایک جرم جس میں کمپیوٹر نیٹ ورک یا آلات کو استعمال کیا جاتا ہے اسے سائبر کرائم کہا جاتا ہے۔

سوال34: سائبر کرائم کی اقسام کون کون سی ہیں؟نام لکھیں۔

جواب: سائبر کرائم کی اقسام مندرجہ ذیل ہیں:

(i)شناخت کی چوری (ii)ٹرانزیکشن فراڈ (iii)ایڈوانس فیس فراڈ

(iv)ہیکنگ (v)پائریسی

سوال35: شناخت کی چوری سے کیا مراد ہے؟

جواب: سائبر کرائم کی ایک عام شکل شناخت کی چوری ہے۔ ہیکرز پاس ورڈ اور اکاؤنٹ کی معلومات حاصل کرنے کے لیے جعلی ای میلز کا استعمال کر سکتے ہیں۔

سوال36: ٹرانزیکشن فراڈ کیا ہے؟

جواب: مالی دھوکا دہی آن لائن میدان میں ایک عام جرم ہے۔ ایک سکیمر(Scammer) ویب سائٹ کے ذریعے فروخت کے لیے کسی چیز کی پیشکش کر سکتا ہے جب کہ وہ ادائیگی وصول کرنے کے بعد آپ کو مطلوبہ چیز نہیں دیتا۔ یہ بھی ممکن ہے کہ آپ اپنے کریڈٹ کارڈ سے کچھ چیزیں خریدیں اور پھر کارڈ چوری کی اطلاع کر دیں۔ اگر کارڈ ہولڈر چارج بیک کا دعویٰ کرتا ہے تو اسے ٹرانزیکشن فراڈ کہتے ہیں۔

سوال37: ایڈوانس فیس فراڈ سے کیا مراد ہے؟

جواب: کبھی کبھی ہیکرز ایک بڑا انعام جیتنے پر آپ کو مبارک باد دیتے ہیں اور پھر آپ کو ایک چھوٹی سی رقم ادا کرنے کے لیے کہتے ہیں تاکہ آپ کو انعام بھیجا جا سکے۔ یہ سائبر کرائم کی ایک عام قسم ہے۔ آسانی سے دولت کمانے کے لالچ کی وجہ سے بہت سارے لوگ اس فراڈ کا شکار ہو جاتے ہیں۔

☆☆☆☆☆

نَحْمَدُهٗ وَ نُصَلِّی عَلٰی رَسُوْلِہِ الْکَرِیْم

معزز اساتذہ کرام، السلام علیکم ورحمۃ اللہ! گزارش ہے کہ سٹوڈنٹس کو مطالعہ سے پہلے درج ذیل دعاؤں کو باقاعدگی سے پڑھنے کی ترغیب دیں۔ جزاک اللہ۔

عزیز طلبا و طالبات، آپ سب بھی دعاؤں کا اہتمام ضرور کریں۔ اللہ تعالیٰ آپ سب کے اور اساتذہ کرام کے علم، زندگی اور ایمان میں برکت دے۔ آمین۔

ہمارے لیے بھی دعا کرتے رہیں۔ اللہ تعالیٰ ہم سب کے لیے دنیا و آخرت میں آسانیاں اور سکون نصیب فرمائے۔

بِسْمِ اللّٰہِ الرَّحْمٰنِ الرَّحِیْمِ ؕ

اللہ کے نام سے شروع جو رحمٰن و رحیم ہے۔

اَللّٰھُمَّ صَلِّ عَلٰی مُحَمَّدٍ وَّعَلٰٓی اٰلِ مُحَمَّدٍ کَمَا صَلَّیْتَ عَلٰٓی اِبْرٰھِیْمَ وَعَلٰٓی اٰلِ اِبْرٰھِیْمَ اِنَّکَ حَمِیْدٌ مَّجِیْدٌ ○ اَللّٰھُمَّ بَارِکْ عَلٰی مُحَمَّدٍ وَّعَلٰٓی اٰلِ مُحَمَّدٍ کَمَا بَارَکْتَ عَلٰٓی اِبْرٰھِیْمَ وَعَلٰٓی اٰلِ اِبْرٰھِیْمَ اِنَّکَ حَمِیْدٌ مَّجِیْدٌ ○

رَبِّ اشْرَحْ لِیْ صَدْرِیْ ○ وَیَسِّرْ لِیْٓ اَمْرِیْ ○ وَاحْلُلْ عُقْدَۃً مِّنْ لِّسَانِیْ ○ یَفْقَھُوْا قَوْلِیْ ○

رَبِّ زِدْنِیْ عِلْمًا۔ رَبِّ زِدْنِیْ عِلْمًا۔ رَبِّ زِدْنِیْ عِلْمًا۔

اَللّٰھُمَّ اِنِّیْٓ اَسْئَلُکَ عِلْمًا نَّافِعًا وَّرِزْقًا طَیِّبًا وَّ عَمَلًا مُّتَقَبَّلًا ○

آخر میں درود شریف دوبارہ پڑھیں۔

اللہ تعالیٰ آپ کو جزا دے، آپ کے علم کے حصول میں آسانیاں عطا فرمائے۔